How To Configure Group Policies to Set Security for System Services

This article was previously published under Q256345

Article ID : 256345
Last Review : October 31, 2006
Revision : 3.2

On This Page

SUMMARY

You can implement security on system services in Windows. This allows you to control who can manage services on a workstation, member server, or domain controller. Currently, the only way to change a system service is through a Group Policy computer setting.

If you implement Group Policy at the Default Domain Policy, the policy takes effect on all computers in the domain. If you implement Group Policy at the Default Domain Controllers policy, the policy only applies to the servers in the domain controller's organizational unit (OU). You can create OUs that contain workstations for which policies can be applied. This article describes the steps to implement a Group Policy on a OU to change permissions on system services.

Steps to Assign System Service Permissions

1. Start **Active Directory Users and Computers**.
2. Right-click the domain in which you want to add the OU, click **New**, and then click **Organizational Unit**.
3. Give the OU an appropriate name, and then click **OK**. The new OU is listed below the domain.
4. Right-click the new OU, and then click **Properties**.
5. The OU properties are now displayed. On the **Group Policy** tab, click **New**. Give the new Group Policy an appropriate name (for example, the name of the OU for which it is implemented).
6. After the policy is created, make sure it is highlighted, and then click **Edit**.
7. Click **Computer Configuration**, click **Windows Settings**, click **Security Settings**, and then click **System Services**.
8. Double-click the service on which you want to apply permissions. The security policy setting for that specific service is displayed.
9. Click to select the **Define this Policy Setting** check box. This action automatically creates security permissions with Everyone having Full Control.
10. Click **Remove** to remove the Everyone group.
11. Click **Add** to add the System account and any other user accounts to which you want to grant access.
12. Set the permission for the System account at Full Control, as well as the appropriate permissions for user accounts or groups. By default, only the start, stop, and pause permissions are granted to all new users.
13. After you finish adding the appropriate users and groups with the appropriate permissions to the service, click **OK**.
14. The service startup mode is set to disabled by default. Change this setting to the correct startup mode (usually automatic).
15. Click **OK**, close the policy, and then click **OK**.

NOTE: You need to move the computer accounts into the OU that you want to manage. After the computer accounts are in the OU, the authorized user or groups in the security permissions can manage the service.

REFERENCES

For additional information about necessary permissions for starting a service, click the article number below to view the article in the Microsoft Knowledge Base:

> 256299 (http://support.microsoft.com/kb/256299/EN-US/) 'Access Denied' Error When Starting a Service in Windows 2000

For additional information about system service permissions not being applied, click the article number below to view the article in the Microsoft Knowledge Base:

> 257247 (http://support.microsoft.com/kb/257247/EN-US/) Policy Changing System Service Permissions Does Not Apply

APPLIES TO

- Microsoft Windows 2000 Server
- Microsoft Windows 2000 Advanced Server
- Microsoft Windows 2000 Professional Edition

Keywords: kbacl kbenv kbgpo kbhowto kbhowtomaster kbsecconfiged KB256345